UNIVERSIDADE NOVA DE LISBOA
Faculdade de Ciências e Tecnologia
Departamento de Informática

Seminários de Informática	Época de Recurso, 21 de Julho de 2006

EXAME

Nome do aluno:_____________________________Nº:_________Curso:_______

IMPORTANTE Duração máxima: 2 horas

O exame é sem consulta, não sendo permitida a utilização de máquinas de calcular. Só é permitido sair, decorrida pelo menos 1 hora após o início do exame, mesmo se pretender desistir. Em qualquer caso é sempre necessário entregar o enunciado do exame.
Se precisar, pode usar o verso das folhas como rascunho.
Para cada pergunta de escolha múltipla, seleccione a resposta que lhe parece mais correcta, mas tenha em conta que cada resposta errada desconta *1/n* do valor da questão, sendo *n* o número de respostas alternativas à pergunta. Todas as questões têm o mesmo valor.
A detecção de fraude implica a reprovação dos alunos envolvidos.

1. A Máquina de Turing
☒ É um modelo abstracto que capta a noção de algoritmo e está presente mesmo nos contextos actuais de computação.
❑ É um formalismo matemático sem qualquer correspondência com os modelos de computação.
❑ Já foi útil mas perdeu utilidade exactamente quando apareceram os computadores pessoais.

2.
☒ Os computadores actuais, conservam a estrutura/filosofia básica da arquitectura de Von Newman.
❑ A arquitectura de Von Newman não tem qualquer correspondência com a arquitectura dos computadores actuais.
❑ A arquitectura de Von Newman deixou de ter qualquer correspondência com a arquitectura dos computadores, quando surgiram os computadores pessoais.

3. Considere o processador P88 usado como exemplo na aula "Arquitectura de Computadores e Sistemas de Operação", as suas instruções máquina e respectivas mnemónicas. Apresenta-se a seguir um programa escrito na linguagem "assembly" do referido CPU:

```
1          in      ax
2          copy    p, ax
3          copy    q, ax
4          add     ax, p
6          out     ax
7          halt
8    p     3
9    q     0
```

Suponha que quando foi executada a instrução 1 o utilizador introduziu no teclado o valor 6 e que antes do programa se iniciar as posições de memória simbolicamente designadas por p e q contêm os valores indicados. Qual o valor de saída produzido na linha 6?

❑ 6
❑ 9
☒ 12

4. Considere o sistema de operação Windows ou Linux (SO) de um computador pessoal. Quando um programa que está a ser executado pretende escrever dados num ficheiro ...

❑ Invoca uma função da biblioteca da linguagem que faz directamente as alterações no disco, sem invocar os serviços do SO.

☒ Invoca uma função da biblioteca da linguagem que por sua vez invoca os serviços do SO e é o SO que efectivamente escreve no disco.

❑ Invoca uma função da biblioteca da linguagem que faz directamente as alterações nos blocos de disco no que diz respeito aos dados, mas para alterar as directorias invoca as funções do SO.

5. Um sistema de gestão de bases de dados deve
☒ evitar redundância de dados para facilitar a verificação de consistência.
❑ permitir redundância de dados para segurança
❑ evitar redundância de dados para facilitar o acesso de programas externos

6. Por um modelo de dados entende-se
☒ Um conjunto de ferramentas formais para descrever dados
❑ Uma base de dados flexível
❑ Um conjunto de dados relacionados em tabelas

7. Qual das seguintes transformações de coordenadas não é considerada uma transformação geométrica elementar?
☒ Perspectiva
❑ Mudança de escala
❑ Rotação

8. Escolha a afirmação que se pode aplicar à técnica designada por "bump mapping":
❑ É um mapeamento de texturas no modelo
☒ Não altera a geometria do modelo
❑ Tem em conta a refracção da luz nos materiais transparentes

9. Foram apresentados na aula dois algoritmos de pesquisa: simples e binária. Ambos algoritmos recebem como "input" (entrada) um vector de números e um número que se pretende encontrar, e como objectivo devolvem verdade ou falso se o mesmo valor se encontra no vector de números. Escolha a afirmação verdadeira:

☒ O algoritmo de pesquisa simples pode funcionar com números ordenados aleatoriamente no vector mas já a pesquisa binária não pode.
❑ A pesquisa simples no caso esperado (O(n/2)) efectua menos passos que a pesquisa binária (O(log n)), significando que é mais rápida.
❑ Os vectores têm de ter tamanhos (complexidade espacial) diferentes para os dois algoritmos.

10. No seminário estudámos o algoritmo de Quicksort e Bubblesort. Nesta aula tivemos a oportunidade de comparar o comportamento dos dois algoritmos de um modo Empírico e de um modo Analítico. Desta maneira temos dois modos fundamentados de fazer a escolha certa. Estudar de um modo analítico é:

☒ Associar ao algoritmo uma função que estime a ordem de grandeza do tempo/espaço.
❑ Medir o tempo/espaço com dados reais.
❑ Medir o tempo/espaço com dados gerados de acordo com determinadas distribuições.

11. O que é um algoritmo?
☒ um conjunto de regras que descrevem uma computação.
❑ um programa informático.
❑ Significa "processamento automático de informação".

12. Por que razão existem tantas linguagens de programação diferentes (por exemplo: Pascal, C, C++, Java, Prolog, Fortran, Lisp) ?

❑ Para ser possível escrever uma maior diversidade de programas, pois há programas que se podem escrever numa determinada linguagem mas não noutra linguagem. Estão constantemente a ser inventadas novas linguagens, com cada vez com maior poder computacional. Assim, vai-se alargando o número de programas que é possível teoricamente escrever.

☒ A generalidade das linguagens de programação são equivalentes entre si do ponto de vista dos programas que se podem teoricamente escrever. Nesta área já está tudo inventado. Estão constantemente a ser criadas novas linguagens com o objectivo de fornecer ao programador novas formas de de exprimir as suas ideias, de forma mais sofisticada e com maior clareza.

❑ Porque, ao longo da história, a generalidade dos fabricantes de computadores foi criando as suas própria linguagens. Esse tipo de actividade tem-se reduzido nos últimos anos.

13. Na *Data Mining*:

❑ Um perceptrão simples deve ser utilizado quando os dados não são linearmente separáveis.

☒ Um perceptrão simples deve ser utilizado quando os dados são linearmente separáveis.

❑ O perceptrão foi desenhado para tratar problemas de segmentação de dados ou clustering.

14. A extracção de conhecimento de uma base de dados:

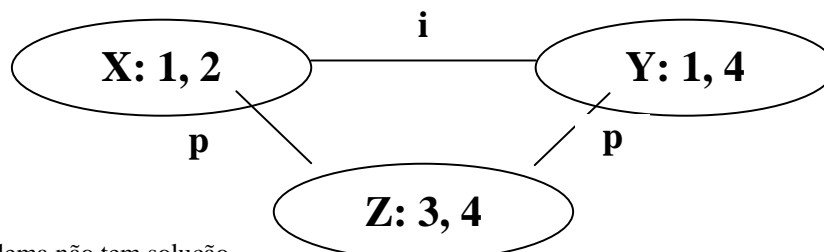
☒É um processo geral que incluí o pré-processamento e limpeza de dados, a agregação de entidades em características a *data mining* para construção de modelos sobre os dados e a interpretação e análise dos modelos gerados para extracção de conhecimentos.
❑ É o processo da data mining que possibilita a construção de grupos de agregação.
❑ É uma etapa do processo de analise de sistemas destinado a construir o modelo entidade relação da base de dados.

15. Num rede de computadores, supondo que apenas existe um possível percurso entre o computador A e B, o tempo de trânsito entre A e B pode variar devido à:
❑ variação do tempo de propagação nos canais de comunicação
❑ variação do tempo de transmissão nos canais de comunicação
☒ variação do tempo "perdido" nas filas de espera dos "routers"

16. Relativamente ao protocolo HTTP, indique qual das seguintes afirmação é FALSA:
❑ usa o protocolo de transporte TCP
❑ é baseado num arquitectura cliente/servidor
☒ é baseado numa arquitectura peer-to-peer

17. Em geral, um sistema de *middleware*:
☒ permite fornecer uma interface homogénea para o desenvolvimento de aplicações
❑ está disponível em apenas uma arquitectura/sistema de operação
❑ apenas executa numa máquina

18. Indique qual das seguintes afirmações **não é verdadeira** relativamente a um proxy:
❑ um proxy pode ser usado para melhorar o desempenho do sistema
❑ um proxy pode ser adicionado a uma arquitectura cliente/servidor
☒ um proxy pode substituir completa e definitivamente um servidor.

19. Considere o seguinte grafo em que os números nos seus vértices só podem tomar os valores indicados (X só pode ser 1 ou 2, Y só pode ser 1 ou 4 e Z só pode ser 3 ou 4) e em que a soma de dois números ligados por um arco deve ser par ou ímpar consoante a etiqueta do arco que os une (X+Y deve ser ímpar, mas X+Z e Y+Z devem ser pares). Utilize a propagação de restrições e diga qual das frases abaixo é correcta.

☒ O problema não tem solução
❑ Existe pelo menos uma solução com X = 1
❑ Não existe uma solução com Y = 1 mas existe com Y = 4.

20. Pretende-se descobrir a melhor maneira de colocar *2N* produtos num saco, mas não é possível colocá-los a todos por excederem o peso que o saco suporta. Considera-se uma solução potencial do problema a selecção de um subconjunto desses produtos (por exemplo, havendo 8 produtos, uma solução potencial é a escolha dos produtos 1, 3, 4 e 8), mesmo que essa solução não seja possível por excesso de peso. Quantas soluções potenciais existem se existirem *2N* produtos?

☒ 2^{2N}
❑ (2N)!
❑ N

21. Apresentam-se a seguir **tipologias de ataques a sistemas de computadores distribuídos suportados em redes de computadores** bem como os termos associados aos **serviços fundamentais de segurança** que estão associados à protecção contra os referidos ataques. Faça corresponder (com setas) os ataques aos serviços de segurança que constituem as contra-medidas para defender os sistemas desses ataques. O significado da correspondência na colocação das setas deve ser: *o Ataque X é protegido pela propriedade de segurança subjacente ao Serviço Y*

Nota: uma seta só pode ligar um ataque a um e um só serviço

X) Ataques:

A
Captura ilícita de mensagens
no canal de comunicação sem
que os principais que estão
nos extremos do canal se apercebam
(*Message-Eavesdropping Attack)*

B
Alteração das mensagens em trânsito
no canal de comunicação sem que as
entidades principais que estão nos extremos
se apercebam
(*Message Tampering Attack*)

C
Um utilizador X envia uma mensagem de
Correio electrónico a um utilizador Y,
com uma declaração de dívida. Mais tarde,
quando Y apresenta a referida mensagem em tribunal
X defende-se dizendo que nunca enviou uma tal
Mensagem e que a mensagem que Y exibe não
é verdadeira e não foi enviada por X.

D
Ataque à memória de um programa executado
num dado computador (pela vítima)
de modo a poder capturar dados que estão
mapeados pelo programa em memória

E
O computador de um atacante é
configurado de modo a apresentar-se numa rede
com um mesmo endereço de um outro computador
(vítima) e assim tentar capturar os dados que seriam
destinados ao computador da vítima

F
Diversos computadores algures na rede internet
enviam uma enorme quantidade de tráfego saturando
a largura de banda (bandwidth) de uma ligação a
um dado servidor WEB e provocando a saturação
do computador em processar adequadamente a
informação que lhe é enviada
(*Distributed Denial of Service Type Attack*)

Y) Serviços

1
INTEGRIDADE
(*Integrity*)

2
AUTENTICAÇÃO
(*Authentication*)

3
CONFIDENCIALIDADE
(*Confidentiality*)

4
CONTROLO DE ACESSOS
(*Access Control*)

5
DISPONIBILIADE
(*Availability*)

6
NÃO REPUDIAÇÃO
(*Non-Repudiation*)

A > 3; B-> 1; C-> 6; D-> 4; E-> 2; F->5.

22. A funcionalidade de LOGIN em que um utilizador precisa de fornecer ao computador informação sobre a identificação de utilizador (*Username ou UserID*) e uma palavra de passe (*password*) para poder usar o sistema e os seus recursos, constitui:

- ☒ Um serviço de Autenticação
- ❑ Um serviço de Controlo de Acessos
- ❑ Um serviço de Integridade
- ❑ Um serviço de Não-Repudiação

23. A Engenharia de Software advoga a adopção de uma aproximação sistemática, disciplinada e quantificável nas seguintes fases do ciclo de vida:

- ❑ da especificação à instalação do software;
- ❑ na operação e manutenção de software;
- ☒ em todas as fases anteriores;

24. O acoplamento é uma característica do desenho de sistemas de software que se refere à forma como os elementos de módulos diferentes estão relacionados. O acoplamento é geralmente considerado uma característica:

- ❑ desejável;
- ☒ indesejável;
- ❑ irrelevante;

25. Os sistemas baseados em conhecimento DENDRAL e MYCIN são:

- ❑ Sistemas Espertos
- ❑ Sistemas Inteligentes
- ☒ Sistemas Periciais

26. O algoritmo de base usado em jogos com adversários é designado:

- ❑ MAXIMIN
- ☒ MINIMAX
- ❑ MINIMIN